

(19)



JAPANESE PATENT OFFICE

JPA 08-221364

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 08221364 A

(43) Date of publication of application: 30.08.96

(51) Int. Cl.

G06F 15/00  
G06F 13/00

(21) Application number: 07026456

(22) Date of filing: 15.02.95

(71) Applicant: HITACHI LTD

(72) Inventor: KOBAYASHI SHIGEYUKI  
HAYASHI TOMONORI  
MORI YASUKO

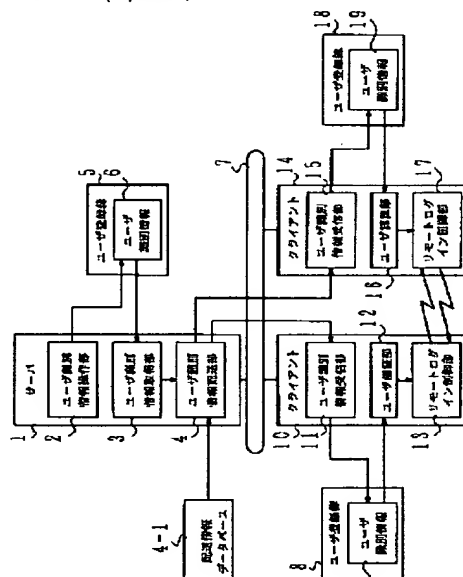
(54) DECENTRALIZED MANAGEMENT METHOD FOR  
USER REGISTRATION BOOK

COPYRIGHT: (C)1996,JPO

(57) Abstract:

PURPOSE: To guarantee the consistency of user identification information among plural systems and to reduce the operation management work for a user registration book on a network system.

CONSTITUTION: A server 1 and clients 10 and 14 constituting a computer system connected through the network system 7 are provided and a means (user identification information operation part 2) for operating the user registration book 5 is present only in the server 1. A user identification information distribution part 4 for distributing the user identification information 6 operated in the server 1 through the network system 7 is present on the server 1, a user identification information reception part 11 is provided on the client 10 and the user identification information reception part 15 is provided on the client 14 for reflecting the distributed user identification information on respective user registration books 8 and 18.



Best Available Copy

JPA08-221364

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-221364

(43) 公開日 平成8年(1996)8月30日

| (51) Int. Cl. <sup>6</sup> | 識別記号 | 庁内整理番号  | F I        | 技術表示箇所 |   |  |
|----------------------------|------|---------|------------|--------|---|--|
| G06F 15/00                 | 330  | 9364-5L | G06F 15/00 | 330    | B |  |
| 13/00                      | 357  | 7368-5E | 13/00      | 357    | Z |  |

審査請求 未請求 請求項の数 1 O L (全7頁)

(21) 出願番号 特願平7-26456

(22) 出願日 平成7年(1995)2月15日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 小林 茂之

神奈川県横浜市戸塚区戸塚町5030番地 株

式会社日立製作所ソフトウェア開発本部内

(72) 発明者 林 朋典

神奈川県横浜市戸塚区戸塚町5030番地 株

式会社日立製作所ソフトウェア開発本部内

(72) 発明者 森 八寿子

神奈川県横浜市戸塚区戸塚町5030番地 株

式会社日立製作所ソフトウェア開発本部内

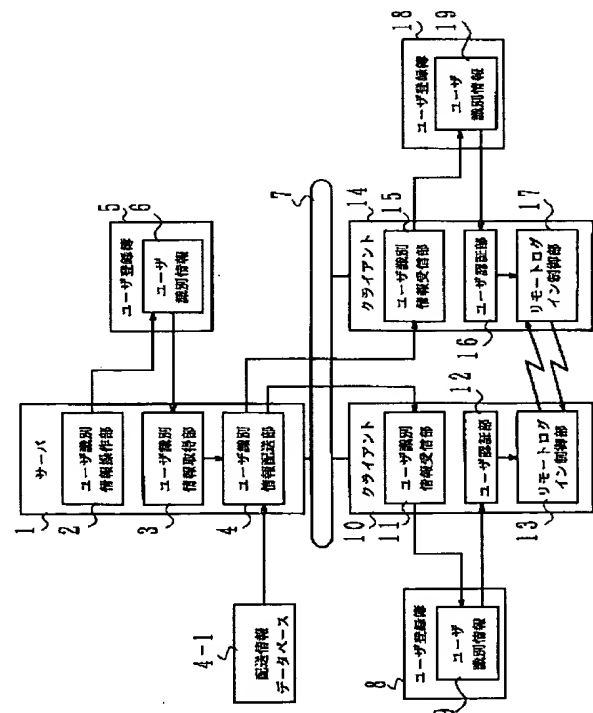
(74) 代理人 弁理士 小川 勝男

(54) 【発明の名称】 ユーザ登録簿の分散管理方法

(57) 【要約】

【目的】複数のシステム間でユーザ識別情報の一貫性を保証するとともに、ネットワークシステム上でのユーザ登録簿の運用管理作業を軽減する。

【構成】ネットワークシステム7を介して接続されたコンピュータシステムであるサーバ1とクライアント10、14があり、ユーザ登録簿5を操作する手段(ユーザ識別情報操作部2)がサーバ1のみに存在し、サーバ1で操作されたユーザ識別情報6をネットワークシステム7を介して配付するユーザ識別情報配送部4がサーバ1上に存在し、配付されたユーザ識別情報をユーザ登録簿8と18にそれぞれ反映するために、クライアント10上にユーザ識別情報受信部11とクライアント14上にユーザ識別情報受信部15を持つ。



**【特許請求の範囲】**

**【請求項 1】** ネットワークシステムを介して複数のコンピュータシステムが接続されたユーザ登録簿の分散管理方法において、

ユーザのリモートログイン操作時に当該ユーザの認証に必要とされるユーザ識別情報を保持するユーザ登録簿を、登録サーバと呼ばれるコンピュータシステムで一元管理するため、

該登録サーバのみがユーザ識別情報を一括操作し、かつ該登録サーバで一括操作された更新ユーザ情報を上記ネットワークシステムを経由して各々のユーザ識別情報を保持するクライアントと呼ばれるコンピュータシステムに配送し、

該クライアントは上記更新ユーザ情報を受け取り、各自が保持するユーザ登録簿に該更新ユーザ情報を登録することを特徴とするユーザ登録簿の分散管理方法。

**【発明の詳細な説明】****【0001】**

**【産業上の利用分野】** 本発明は、ネットワーク分散環境におけるユーザ登録簿の分散管理方法に関し、特に複数コンピュータ相互間でリモートログインを許可するか否かの手続きを単純化し、かつユーザ認証情報の一貫性を保証することができるユーザ登録簿の分散管理方法に関する。

**【0002】**

**【従来の技術】** 近年、ネットワークシステムを介してワークステーションからパーソナルコンピュータ、メインフレーム等のコンピュータシステムを接続し、大規模なシステムを構築する場合が増加している。このような環境の中で、これらのシステム相互間でリモートログイン等のサービスを提供するためには、ユーザ登録簿によるユーザの認証が必要である。なお、リモートログインとは、複数のコンピュータが相互接続されている場合に、1つのコンピュータを介して他のコンピュータのプログラムやデータを使用することであり、その際の認証とは、あるユーザが常時使用しているコンピュータ A を経由して他のコンピュータ B を使用する際に、そのコンピュータ B の使用を要求することにより、そのコンピュータ B がそのユーザを使用させてよいか否かを許可する手続きを言う。この場合、一般に個々のコンピュータシステムでユーザ登録簿を管理することによる管理作業の増大が問題となっている。

**【0003】** 図 2 は、従来のネットワークシステム上で行われているユーザ登録簿の管理方法の例を示す図である。図 2 では、サーバ 20、クライアント 27、28 の 3 つのコンピュータシステムがネットワークシステム 26 で接続されている。これらの 3 つのコンピュータシステムでは、共通なユーザ識別情報 25 がユーザ登録簿 24 に保持されており、サーバ 20 のみがユーザ登録簿 24 を操作することができる。サーバ 20 はユーザ登録簿

10

20

30

40

50

24 中のユーザ識別情報の一部または全てに対して、追加、削除、更新などの操作を行うために必要なユーザ識別情報操作部 21 を有する。いま、クライアント 27 のリモートログイン制御部 31 がユーザの指示によってクライアント 28 にリモートログインしようとする場合、リモートログイン制御部 31 はクライアント 28 上のリモートログイン制御部 34 とネットワークシステム 26 を介して接続される。クライアント 28 上のリモートログイン制御部 34 は、クライアント 27 上のリモートログイン制御部 31 からログインを要求するユーザを認証するため、ユーザ認証部 33 を呼び出す。ユーザを認証するためのユーザ識別情報 25 はサーバ 20 に接続されたユーザ登録簿 24 上にのみ存在するため、クライアント 28 のユーザ認証部 33 はユーザ識別情報要求部 32 を呼び出す。ユーザ識別情報要求部 32 はネットワークシステム 26 を介して、サーバ 20 上のユーザ識別情報管理部 23 と通信し、ユーザ識別情報管理部 23 はユーザ識別情報取得部 22 を呼び出し、ユーザ登録簿 24 から当該ユーザのユーザ識別情報を得る。クライアント 28 のユーザ認証部 33 は、取得したユーザ識別情報を元にクライアント 27 のユーザを認証し、リモートログインを許可するか否かを決定する。なお、クライアント 28 上のユーザがクライアント 27 にリモートログインする時も、全く同様の手続きを行うことにより、ユーザ登録簿 24 の保持するユーザ識別情報 25 をサーバ 20 に問い合わせ、リモートログインを許可するか否かが決定される。この方法では、リモートログイン時のユーザ認証のために、サーバへの問い合わせが必須となる。

**【0004】** 図 3 は、他の従来例を示すもので、ユーザ登録簿を個々のホストで別々に管理する場合を示している。図 3 では、ホスト 35、44、48 の 3 つがネットワークシステム 41 を介して接続されており、それぞれのホストにユーザ登録簿 39、42、52 が接続されている。これらの 3 つのユーザ登録簿 39、42、52 には、ユーザ識別情報 40、43、53 がそれぞれ保持されており、また各ホストは、各々のユーザ識別情報の一部または全てに対して、追加、削除、更新などの操作を行うために必要なユーザ識別情報操作部 36、47、51 の 3 つを備えている。ホスト 35 のリモートログイン制御部 38 が、ユーザの指示によってホスト 44 にリモートログインしようとする場合、リモートログイン制御部 38 はホスト 44 上のリモートログイン制御部 45 とネットワークシステム 41 を介して接続される。ホスト 44 上のリモートログイン制御部 45 は、リモートログイン制御部 38 からログインを要求するユーザを認証するため、ユーザ認証部 46 を呼び出す。ユーザ認証部 46 ではユーザ登録簿 42 に保持されたユーザ識別情報 43 から当該ユーザのユーザ識別情報を取得し、ホスト 35 上のユーザを認証し、リモートログインを許可するか否かを決定する。この方法では、ホスト毎にユーザ登録

簿が保持され、リモートログインが要求されたホスト上で、リモートログインを要求するユーザの認証が行われる。なお、この種のネットワーク上でのユーザ登録簿の管理方法については、例えば「SUNシステム管理」

(株式会社アスキー 平成3年3月20日発行)のP. 203からP. 207までに記載されている。

#### 【0005】

【発明が解決しようとする課題】図2で例示される従来の方法では、クライアントシステム27や28がリモートログインを要求するユーザを認証するためには、サーバ20にネットワークシステム26を介して問い合わせる必要があった。このため、サーバ20が故障などの原因で使用不可能になると、ネットワークシステム26に接続されたクライアント27、28、サーバ20の相互のコンピュータシステム間で、リモートログイン機能が全く使えなくなるという弱点があった。また、この従来方法では、管理されるコンピュータシステムの数が増加すると、サーバ20への問い合わせ数が増大し、ネットワークシステム26上のネットワーク性能に悪影響を与えるとともに、システムの可用性を低下させる場合があるという問題点があった。図3で例示される従来の方法では、ユーザ識別情報が個々のホストで別々に管理されているため、ネットワーク上でのユーザ認証情報の一貫性を保つためには、同じユーザの認証情報をそれぞれのユーザ登録簿に別々に登録する必要があるという無駄があった。つまり、ユーザ識別情報の操作が必要な場合には、ホスト35、44、48のそれぞれでユーザ識別情報操作部36、47、51を使用して、ユーザ識別情報40、43、53を更新する必要があった。従って、ネットワークシステム41に接続されるホスト数が増加するに伴って、ユーザ識別情報の更新に必要な管理作業も増加するという問題があった。本発明の目的は、このような従来の課題を解決し、複数ホストに対するユーザ認証情報の一貫性を保証することができるとともに、複数ホストのユーザ登録簿を更新するための作業を軽減することができるユーザ登録簿の分散管理方法を提供することにある。

#### 【0006】

【課題を解決するための手段】上記の目的を達成するため、本発明によるユーザ登録簿の分散管理方法では、ユーザ識別情報を操作するための唯一の手段であるユーザ識別情報操作部をネットワークシステム上の一つのサーバのみに置き、ユーザ識別情報操作部からの指示により、更新されたユーザ識別情報をユーザ識別情報配送部から配送し、ユーザ識別情報受信部がユーザ識別情報配送部からユーザ識別情報を受け取り、ユーザ登録簿に登録することによって、ユーザ識別情報を一括管理する。また、それぞれのホストに接続されたユーザ登録簿の情報でユーザを認証することによって、サーバへの問い合わせのためのトラヒック量を削減することができる。

#### 【0007】

【作用】本発明においては、ユーザ識別情報を操作するユーザ識別情報操作部をネットワークシステム上の一つのサーバのみに配置することにより、ネットワークで接続された複数のコンピュータでユーザの認証のために使われるユーザ識別情報をサーバで一括して操作することを可能としている。また、サーバで操作されたユーザ識別情報をネットワークで接続されたコンピュータシステムに配布する手段をサーバに持たせることによって、各コンピュータのユーザ登録簿にユーザ識別情報を配布することを可能にしている。この結果、ユーザ登録簿をそれぞれのコンピュータシステムで別々に管理する場合に比べて、ユーザ登録簿の運用管理にかかる作業を軽減することができる。また、リモートログイン時のユーザの認証において、それぞれのコンピュータに独立して配置されたユーザ登録簿中のユーザ識別情報を元に当該ユーザを認証することによって、ネットワークシステムのサーバなどに依存すること無く、ネットワーク上の個々のコンピュータシステムで、独立してユーザの認証を可能としている。この結果、本発明では、リモートログインを要求するユーザを認証する時に、サーバにのみユーザ登録簿を配置する方法に比べて、クライアントコンピュータからサーバへのネットワーク経由で通信する処理を無くすることができ、サーバの障害発生によりリモートログインサービスが使用出来なくなるような不都合を無くすることができる。

#### 【0008】

【実施例】以下、本発明の実施例を、図面により詳細に説明する。図1は、本発明の一実施例を示すユーザ登録簿の分散管理システムの構成図である。図1では、サーバ1、クライアント10、クライアント14の3つのコンピュータシステムが、ネットワークシステム7で接続されている。ユーザ登録簿5、8、18は、サーバ1、クライアント10、クライアント14でそれぞれ別々に保持されている。図3に示す従来方法との違いは、図3ではユーザ登録簿中のユーザ識別情報を操作するための手段であるホスト35、ホスト44、ホスト48がユーザ識別情報操作部36、47、51をそれぞれ別々に保持していたのに対し、図1では、ユーザ識別情報操作部36がホスト35にのみ保持されている点である。これを、図3に適用すると、ユーザ登録簿39、42、52中のユーザ識別情報40、43、53の管理をすべてホスト35のユーザ識別情報操作部36により実施することを意味する。但し、図1では、ユーザ登録簿5、8、18中のユーザ識別情報6、9、19の一貫性を保つため、サーバ1のユーザ識別情報操作部2で操作されたユーザ識別情報6を配布するための手段として、サーバ1はユーザ識別情報取得部3とユーザ識別情報配送部4を持っている。また、サーバ1から配送されるユーザ識別情報を受け取り、ユーザ登録簿8と18に反映するため

に、クライアント 10 と 14 はそれぞれユーザ識別情報受信部 11 と 15 を持っている。

【0009】まず、ユーザ識別情報の操作は、サーバ 1 上のユーザ識別情報操作部 2 の指示によって、ユーザ登録簿 5 中にユーザ識別情報 6 として反映される。次に、サーバ 1 のユーザ識別情報取得部 3 は前記操作で更新されたユーザ識別情報 6 をユーザ識別情報配送部 4 に渡す。ユーザ識別情報配送部 4 は、配送情報データベース 4-1 の情報を参照し、ユーザ識別情報を配送すべきホストとしてクライアント 10 と 14 を探しだし、ネット  
10 ワークシステム 7 を介してユーザ識別情報 6 を、クライアント 10 のユーザ識別情報受信部 11 と、クライアント 14 のユーザ識別情報受信部 15 にそれぞれ渡す。ユーザ識別情報を受け取ったクライアント 10 とクライアント 14 のユーザ識別情報受信部 11 と 15 は、それぞれユーザ登録簿 8 とユーザ登録簿 18 にその情報を反映する。このようにして、サーバ 1 上だけでユーザ識別情報の操作を可能にするので、サーバ 1、クライアント 10、クライアント 14 のユーザ識別情報 6、9、19 の一貫性を保つことが可能となる。

【0010】4 図は、ユーザ識別情報の配送を制御するための配送情報データベースの一例を示すフォーマット図である。4 図で示されるように、配送情報データベース 4-1 には、ユーザ毎にビット 0 からビット n までのビットマップをテーブルとして持っている。各ビットは、本発明でユーザ登録簿を管理するホストに対応している。つまり、ビット 0 はホスト A、ビット 1 はホスト B、ビット 2 はホスト C、ビット 3 はホスト D、ビット n はホスト n のように対応する。ビット 0 ~ n の位置に  
30 ‘1’ が立っているときユーザが使用できるコンピュータを持つホストであり、‘0’ が立っているときユーザが使用できないコンピュータを持つホストであることを意味している。例えば、ユーザ A (54) は、ホスト B、ホスト E を使用できること、ユーザ B (55) はホスト A、ホスト E を使用できること、ユーザ C (56) は、ホスト C、ホスト D、ホスト E を使用できること、ユーザ D (57) は、ホスト A ~ ホスト n までの全ホストを使用できることをそれぞれ表わしている。

【0011】従って、システム側から見た場合におけるそれぞれのビットの意味は、当該ユーザ名のユーザ識別情報に変更がなされた場合に、当該ユーザのユーザ識別情報を配送すべきホストかどうかを示している。例えば、ビット 0 が 1 であるならば、ホスト A にユーザ識別情報を配送する必要があることを示し、ビット 0 が 0 であるならば、ホスト A にユーザ識別情報を配送する必要がないことを示す。本実施例では、ユーザ A 54、ユーザ B 55、ユーザ C 56、ユーザ D 57 が図 4 に明示されている。そして、ユーザ A はビット 0 が 0、ビット 1 が 1、ビット 2 が 0、ビット 3 が 0、ビット 4 が 1 であり、ビット n が 0 であることが図 4 に示されている。こ  
40 50

のことは、ユーザ A 54 のユーザ識別情報がサーバ 1 で変更された場合、ビット 1 が 1 であるホスト A とビット 4 が 1 であるホスト D にユーザ A 54 のユーザ識別情報を配送するというを示す。

【0012】次に、本実施例におけるリモートログイン時のユーザの認証については、図 3 で示された従来方法と同等の方法で実現する。図 1 では、クライアント 10 上のユーザがクライアント 14 にリモートログインしようとする場合には、クライアント 10 のリモートログイン制御部 13 がユーザの指示によって、クライアント 14 にリモートログインしようとする場合、リモートログイン制御部 13 はクライアント 14 上のログイン制御部 17 とネットワークシステム 7 を介して接続される。クライアント 14 上のリモートログイン制御部 17 は、リモートログイン制御部 13 からログインを要求するユーザを認証するために、ユーザ認証部 16 を呼び出す。ユーザ認証部 16 ではユーザ登録簿 18 に保持されたユーザ識別情報 19 から当該ユーザのユーザ識別情報を取得し、クライアント 10 上のユーザを認証し、リモートログインを許可するか否かを決定する。この方法では、ホスト毎にユーザ登録簿が保持され、リモートログインが要求されたホスト上でユーザの認証が行われるため、図 2 で示された方法のようなサーバへの問い合わせによるネットワークトラフィック量の増加や、リモートログインができなくなるといった問題を解消することができる。

#### 【0013】

【発明の効果】以上説明したように、本発明によれば、ネットワークシステム上で複数のホストに接続されたユーザ登録簿の更新情報を各ホストに配布する唯一の手段を設けたため、複数ホストに対するユーザ認証情報の一貫性を保証することができ、かつサーバへの問い合わせ数も増大することなく、複数ホストのユーザ登録簿を更新するための作業を軽減するという効果を有する。

#### 【図面の簡単な説明】

【図 1】本発明の一実施例を示すユーザ登録簿分散管理システムの構成図である。

【図 2】従来例を示すものであって、サーバでユーザ登録簿を管理し、クライアントとサーバの協調によりユーザを認証するシステムの構成例図である。

【図 3】従来例を示すものであって、各ホストで別々にユーザ登録簿を管理し、各ホストでユーザを認証するシステムの構成例図である。

【図 4】図 1 におけるユーザ識別情報の配送に使用される配送情報データベースの内容の一例を示す図である。

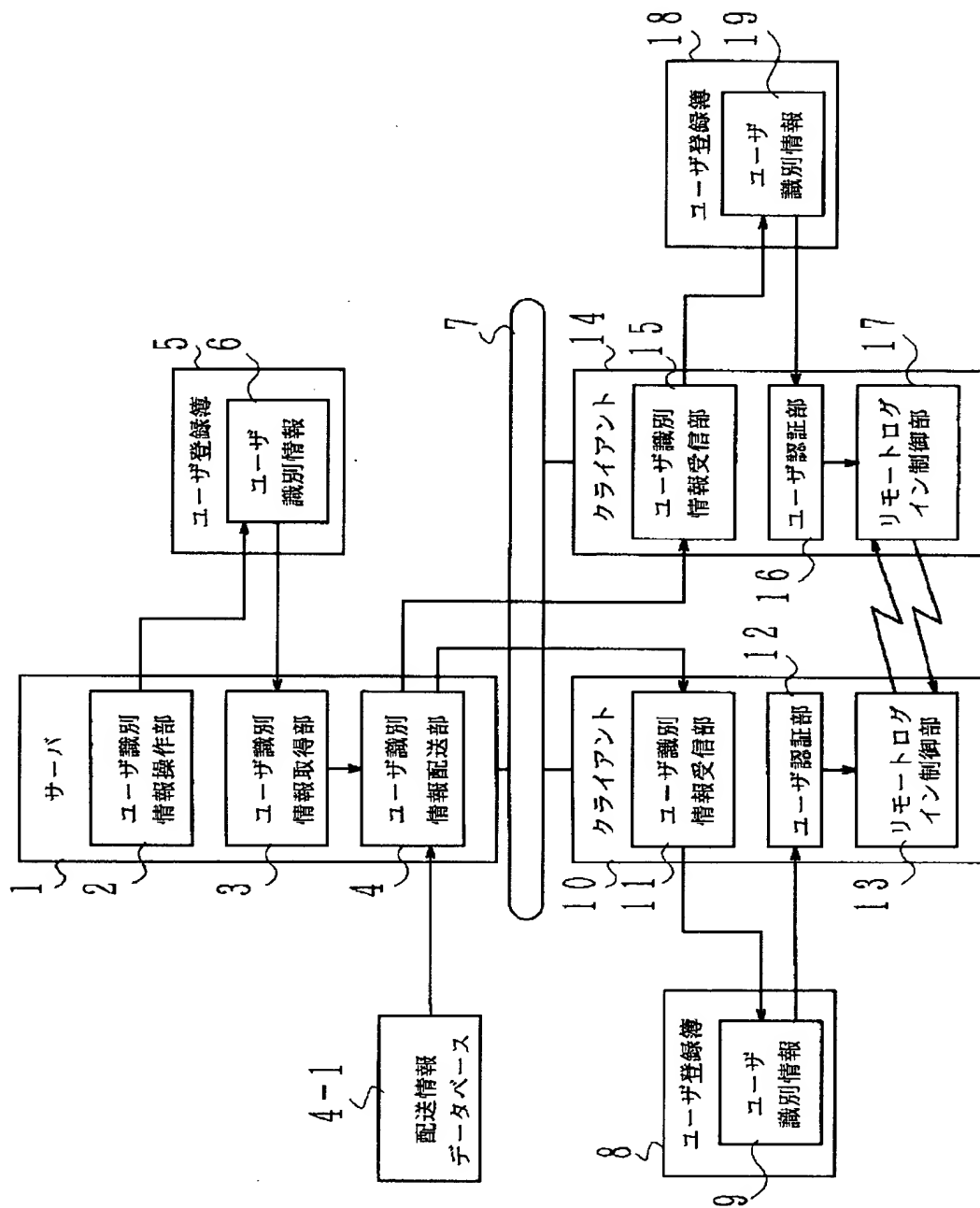
#### 【符号の説明】

1…サーバ、2…ユーザ識別情報操作部、3…ユーザ識別情報取得部、4…ユーザ識別情報配送部、5, 8, 18…ユーザ登録簿、6, 9, 19…ユーザ識別情報、7…ネットワークシステム、8…ユーザ登録簿、10, 14…クライアント、11, 15…ユーザ識別情報受信

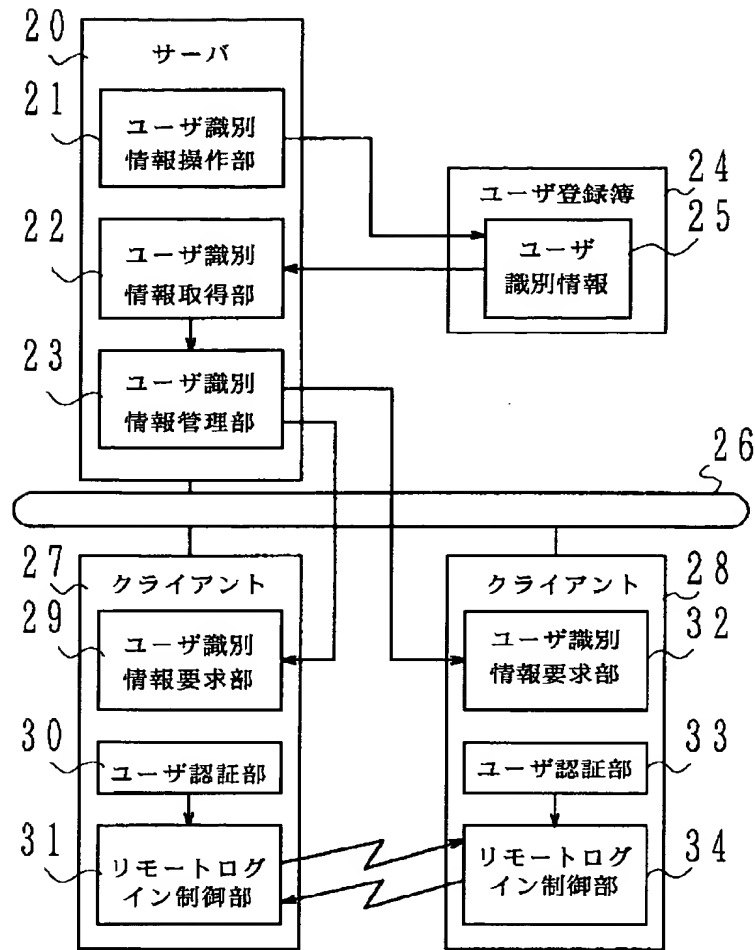
部、12, 16…ユーザ認証部、13, 17…リモート  
ログイン制御部、4-1…配送情報データベース、20

…サーバ、27, 28…クライアント、35, 44, 4  
8…ホスト。

【図1】



【図 2】



【図 4】

58 配送情報データベース

|       | ホスト A | ホスト B | ホスト C | ホスト D | ホスト E | ... | ホスト n |
|-------|-------|-------|-------|-------|-------|-----|-------|
| ビット   | 0     | 1     | 2     | 3     | 4     |     | n     |
| ユーザ A | 0     | 1     | 0     | 0     | 1     |     | 0     |
| ユーザ B | 1     | 0     | 0     | 0     | 1     |     | 0     |
| ユーザ C | 0     | 0     | 1     | 1     | 1     |     | 0     |
| ユーザ D | 1     | 1     | 1     | 1     | 1     |     | 1     |
| ⋮     |       |       |       |       |       |     |       |

【図 3】

